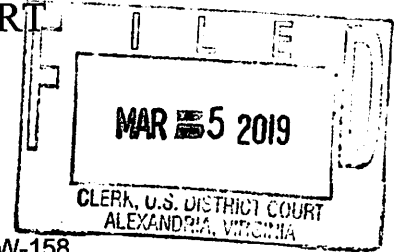


## UNITED STATES DISTRICT COURT

for the  
Eastern District of Virginia



In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

2750 GALLOWS ROAD APARTMENT 401  
VIENNA, VIRGINIA

Case No. 1:19-SW-158

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

2750 GALLOWS ROAD APARTMENT 401, VIENNA, VIRGINIA, as described in Attachment.

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized):

See Attachment.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 201	Bribery;
18 U.S.C. § 371	Conspiracy;
18 U.S.C. § 922	Firearms Dealing.

The application is based on these facts:

☒ Continued on the attached sheet.


☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

SAUSA Brendan Geary/AUSA Jonathan L. Fahey

Sworn to before me and signed in my presence.

Date: 3/5/19

City and state: Alexandria, Virginia

  
Applicant's signature

Jeffrey Scott, Special Agent, FBI

Printed name and title

/s/

 Theresa Carroll Buchanan  
United States Magistrate Judge

Judge's signature

Hon. Theresa Carroll Buchanan, U.S. Magistrate Judge

Printed name and title

**ATTACHMENT A**

*Property to be searched*

The property to be searched is 2750 Gallows Road Apartment 401, Vienna, Virginia (the "PREMISES"), further described as an apartment on the fourth floor of an apartment building. The apartment itself has a brown door with the number 401 on the wall to the left of the door. The apartment building has the name "AVALON" above the main entrance and on the glass wall next to the main entrance below the number 2750.



**ATTACHMENT B**

*Property to be seized*

1. The items to be seized are fruits, evidence, information, contraband, or instrumentalities, in whatever form and however stored, relating to violations of Title 18 United States Code Sections 201, 371, and 922 as described in the search warrant affidavit, including, but not limited to:

- a. Records and information relating to firearm(s) and/or gun(s), purchasers of firearm(s) and/or gun(s), and/or suppliers of firearm(s) and/or gun(s) including but not limited to firearm(s) and/or gun(s) themselves and/or photo(s) of firearm(s) and/or gun(s).
- b. Records and information relating to law enforcement officer(s) or employee(s) of a law enforcement agency/department;
- c. Records and information relating to the contact Jay Dc (believed to be Jason Last Name Unknown (LNU)), the contact A. Dc Cop (believed to be Alex LNU), Jason LNU, Alex LNU, Serge LNU (believed to be Sergei Kazarian), Nate LNU, or Layth LNU (believed to be Layth Mansour);
- d. Records and information relating to the identity or location of perpetrators, aiders and abettors, coconspirators, and accessories after the fact;
- e. Records and information that constitute evidence of use, control, ownership, or occupancy of the PREMISES and things therein;
- f. Records and information that constitute evidence of the state of mind of Nemanja Brankovic, Jason LNU, Alex LNU, Serge LNU (believed to be Sergei Kazarian),

Nate LNU, and/or Layth LNU (believed to be Layth Mansour), *e.g.*, attempts to delete communications and/or contact information, intent, absence of mistake, or evidence indicating preparation or planning, or knowledge and experience, related to the criminal activity under investigation; and

- g. Records and information that constitute evidence concerning persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with Nemanja Brankovic, Jason LNU, Alex LNU, Serge LNU (believed to be Sergei Kazarian), Nate LNU, and/or Layth LNU (believed to be Layth Mansour), about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts.
2. Digital devices used in the commission of, or to facilitate, the above described offenses, including facilitating or attempting to facilitate the illegal transfer of firearms in violation of 18 U.S.C. § 922.

3. For any digital device which is capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities as described in the search warrant affidavit and above, hereinafter the “Device(s)”:

- a. evidence of who used, owned, or controlled the Device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, chat, instant messaging logs, photographs, and correspondence;

- b. evidence of software, or the lack thereof, that would allow others to control the Device(s), such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the attachment to the Device(s) of other storage devices or similar containers for electronic evidence;
- d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Device(s);
- e. evidence of the times the Device(s) was used;
- f. passwords, encryption keys, and other access devices that may be necessary to access the Device(s);
- g. documentation and manuals that may be necessary to access the Device(s) or to conduct a forensic examination of the Device(s);
- h. records of or information about Internet Protocol addresses used by the Device(s);
- i. records of or information about the Device(s)'s Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
- j. Information that constitutes evidence concerning persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with the

Account about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts;

- k. Information that constitutes evidence indicating the Account user's state of mind, *e.g.*, attempts to delete communications and/or contact information, intent, absence of mistake, or evidence indicating preparation or planning, related to the criminal activity under investigation;
- l. Information that constitutes evidence concerning how and when the Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the Account user;
- m. Records and information (to include iMessages, SMS messages, MMS messages, instant messages, emails, including stored or preserved copies of communications (including all draft and deleted messages and deleted contacts)) relating to:
  - i. Firearm(s) and/or gun(s), purchasers of firearm(s) and/or gun(s), and/or suppliers of firearm(s);
  - ii. Photo(s) of firearm(s) and/or gun(s);
  - iii. Photo(s) of law enforcement officer(s) or employee(s) of a law enforcement agency/department;
  - iv. Photo(s) of Jay Dc (believed to be Jason Last Name Unknown (LNU)), A. Dc Cop (believed to be Alex LNU), Jason LNU, Alex LNU, Serge LNU (believed to be Sergei Kazarian), Nate LNU, or Layth LNU (believed to be Layth Mansour);

- v. Communications with, including, and/or about Jay Dc (believed to be Jason Last Name Unknown (LNU)), A. Dc Cop (believed to be Alex LNU), Jason LNU, Alex LNU, Serge LNU (believed to be Sergei Kazarian), Nate LNU, or Layth LNU (believed to be Layth Mansour);
- vi. Communications with current and/or former employee(s) of the District of Columbia Metropolitan Police Department;
- vii. Communications with, including, and/or about law enforcement officer(s), or employee(s) of a law enforcement agency/department;
- viii. The solicitation, request, offer, promise, gift, provision, demand, acceptance, or receipt of any bribes, or any agreement related thereto;
- ix. The identity and/or location of perpetrators, aiders and abettors, and co-conspirators;
- x. Names, addresses, telephone numbers, e-mail addresses, social media accounts, and any other user profiles of perpetrators, aiders and abettors and co-conspirators; and
- xi. Any motive for committing the above named offenses.

4. During the execution of the search of the PREMISES described in Attachment A, law enforcement personnel are also specifically authorized to obtain from Nemanja Brankovic (but not any other individuals present at the PREMISES at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock any Device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable

suspicion that the aforementioned person(s)' physical biometric characteristics will unlock the Device(s), to include pressing fingers or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition of:

- (a) any of the Device(s) found at the PREMISES,
- (b) where the Device(s) are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the Device(s)'s security features in order to search the contents as authorized by this warrant.

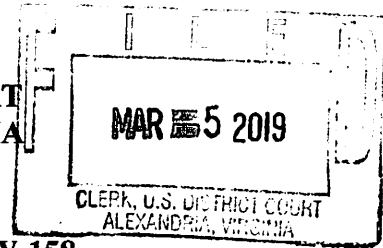
5. While attempting to unlock the device by use of the compelled display of biometric characteristics pursuant to this warrant, law enforcement is not authorized to demand that the aforementioned person(s) state or otherwise provide the password or identify the specific biometric characteristics (including the unique finger(s) or other physical features), that may be used to unlock or access the Device(s). Nor does the warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) is permitted. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person(s) for the password to any Device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device(s), the agents will not state or otherwise imply that the warrant requires the person to

provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

6. As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

7. The term “digital devices” includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); security devices; and any other type of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions.

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA**



**IN THE MATTER OF THE SEARCH OF:  
2750 GALLOWS ROAD APARTMENT 401  
VIENNA, VIRGINIA UNDER RULE 41**

**SW No. 1:19-SW-158**

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41  
FOR A WARRANT TO SEARCH AND SEIZE**

I, Jeffrey Scott, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 2750 Gallows Road Apartment 401, Vienna, Virginia, hereinafter the "PREMISES," further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). I have been in this position since April 2010. Since April 2010, I have been assigned to the FBI Washington Field Office's District of Columbia public corruption squad. Prior to becoming a Special Agent, I was an Intelligence Analyst in the Public Corruption/Civil Rights Intelligence Unit of the FBI from June 2004 until I began my training as a Special Agent in December 2009. During my employment with the FBI, I have conducted and/or assisted in many criminal investigations involving public corruption, fraud, false statements, and other related federal violations. I have training and experience in the enforcement of the laws of the United States, including the preparation and presentation of affidavits in support of warrants. Among other things, I have had both training and experience in the investigation of computer-related crimes

and have worked with other FBI agents who have such experience, and who have provided me with additional information about such crimes. As a federal agent, I am authorized to investigate violations of laws of the United States, and as a law enforcement officer I am authorized to execute warrants issued under the authority of the United States.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that violations of Title 18 United States Code Sections 201 (bribery), 371 (conspiracy), and 922 (firearms dealing), have been committed by Jason Last Name Unknown (LNU) ("Jason LNU"), Serge LNU ("Serge LNU") (believed to be Sergei Kazarian), Nate LNU ("Nate LNU"), Alex LNU ("Alex LNU"), and Nemanja Brankovic, also known as Fabio ("Brankovic"). There is also probable cause to search the PREMISES, further described in Attachment A, for the things described in Attachment B.

#### **PROBABLE CAUSE**

5. Confidential Human Source ("CHS") works in the nightclub industry in the District of Columbia. Brankovic previously worked as a promoter at District of Columbia area nightclubs. CHS and Brankovic are close associates. CHS is also the subject of an ongoing public corruption investigation, and on January 17, 2019, CHS pled guilty to one count of bribery of a public official in violation of 18 U.S.C. § 201 pursuant to a cooperation plea agreement. Under the terms of that agreement, if the government decides that CHS has provided

substantial assistance to the investigation, the government will not oppose CHS's motion for a downward departure from the applicable Sentencing Guidelines range. In the course of his/her cooperation with the investigation, CHS has consistently provided truthful information to law enforcement agents.

6. On August 17, 2018, as part of his cooperation with the investigation, CHS made a consensually recorded telephone call to Brankovic at telephone number 202-997-5531, regarding obtaining a gun from a District of Columbia police officer. Sometime prior to the call on August 17, 2018, Brankovic had mentioned the possibility of obtaining a gun from a police officer for CHS and CHS brought up this topic again on the call.

7. During the call on August 17, 2018, the following conversation between CHS and Brankovic ("NB") occurred:

CHS: ...you said your boy can get me the gun or no you think

NB: What

CHS: Just a gun to have

NB: Yeah

...

CHS: ...if your boy can get one it'd be great...or just be hard to get from him

NB: Well, I'll ask around, I tell you whats, what they have, then I'll send you pictures

CHS: ...is it a cop guy you think, or is he legit or just bullshit

NB: no, legit guns bro

CHS: Huh

NB: They're legit guns

CHS: I know but I'm saying it's not some shit that somebody got you know, killed somebody with or something

NB: Well, you, you can't track them that's the thing, I don't know

CHS: How can they not track them

NB: I guess on some of the guns they erase the, the barcodes, you know, they, they burn them with acid so the gun has no trace, you know, just in case someone, someone gets killed you know [laughs]

CHS: But, But I'm saying this things are not coming from wackos, they're coming from a cop or something

NB: No man, no man, I get them, honestly bro, Layth has them

CHS: Oh Layth has them

NB: Yeah

CHS: And he, and he has a, and he can just get them, but I don't want to get something that you know oh fuck, this motherfucker, this gun killed twenty people with it

NB: Well, [unintelligible] honestly you do not know, honestly

CHS: Where it came from

NB: Yeah, you don't

CHS: Right, but he, but that guy has it, but he definitely has it

NB: Yeah

CHS: [unintelligible]

NB: It might take him like you know, I'll ask around and let you know, I'll ask him, obviously I got to ask him, listen I can't get any of that baller shit, let me see it

...

CHS: ...I thought one of the, the gun stuff was mostly from a cop guy, but not, but it's not, it's mostly, this is from him

NB: Bro, I, bro, you know who the cop guy is

CHS: Uh-un

NB: You know the guy Jason that [unintelligible] at Decades, the white guy

CHS: Jason, no

NB: You know him, he say hi when I'm there when you're there

CHS: The, the really nice white guy

NB: Yeah

CHS: At the door, yeah I think, what's his name

NB: Uh, Jason

CHS: Jason, I think so, he's like Spanish or something, right

NB: No, [unintelligible] white

CHS: Huh

NB: He thinks he's white

CHS: He's white, but, the cop guy

NB: Yeah, he works, he's a DC guy

CHS: Yeah, yeah, he can get that shit

NB: Yeah

CHS: So weird I wouldn't even think twice that that guy would have them, but he doesn't work in, how does he, he doesn't work in the criminal side

NB: But, I'm sure he knows someone that does

CHS: Oh you know

NB: [Unintelligible]

CHS: How did you, how did you know him

NB: Bro I know him from, first time when I, he was friends with Cindy, like seven eight years ago when I started dating Cindy you know

CHS: He was banging Cindy

NB: No, no, I met him through Cindy, he was Cindy's friend, that's the first time when I met Cindy started hanging out with her, then I met this guy because he was always

coming to Camelot and then sometimes Cindy gets fucked up, he's escorting her, you know what I'm saying [laughing]

CHS: Oh I see, but he's, he's the super nice guy that always saying hi and whatever

NB: No he's a great guy, he's a great guy, yeah

CHS: So he must know somebody in in that area

NB: Yeah

CHS: But you never, you never gotten it from him

NB: No, no, I never, I never owned a gun

CHS: No but I'm saying, but how would you, how do you know he's gonna, he's good for it

NB: Huh, because he gets a few guys, he, he give it to Nate, he give it to Serge

CHS: Ah, okay, and they're, they're legit

NB: Yeah

...

CHS: ...even not for me, not even for me, I'm saying this idiot always asks me for, I'm like dude if they need them, maybe they can make money from this guy, I don't give a shit, but I don't want to get, I'm sure the guy won't do it for anybody, you know

NB: No, if it's [unintelligible], for you because like you have a valid reason to have it, you have a big house, you by yourself, like you know, it's kind of, this and that, let's say god forbid you have to use it, you know what I'm saying if it's not legal [unintelligible]

CHS: But what how, why does this moron give it to those idiots, those idiots are the highest risk people to get

NB: Ah who

CHS: To those two people you said, the, what's his name, fuckin that crack head

NB: Layth

CHS: No, the guys that you said

NB: Albert

CHS: No you said he got it for Serge and those guys [laughs], why would he do that

NB: Well, we'll they're friends

CHS: Yeah

NB: They're friends, you know

CHS: Yeah but if something happens it not going to come back to him, you know

NB: Well that's, that's, I don't know, I don't know, we definitely [unintelligible]

CHS: That's what I'm saying, but, but I'm saying if there is somebody who wants it would he do it, or he wouldn't do it for them, he would just do it for somebody else

NB: No, well I, yeah I mean

CHS: You never know

NB: I would say like you know, if, if, if you ask right like you know [unintelligible]

CHS: He's not doing it for money, is what I'm saying

NB: No, no, hell no, no, no, uh uh, uh uh, it's not like, it's not like, it's [laughs] bro it's not like [laughs], it's not like he's selling them for no, not like that, he can get it under the table, no one needs to know, like you know it's, it's kind of discrete you know

CHS: Alright, so he's got to know somebody in, in DC that gets them

NB: Yeah, yup  
CHS: And they nice  
NB: Huh  
CHS: They're nice  
NB: Well not, not necessarily  
CHS: [laughs]  
NB: Not necessarily, they're all beat up, bro, depends, depends what kind of luck you got, because  
CHS: Alright  
NB: Remember it's not listen they're like they're agency they're like everything is in black market, it's not like you go in a store and then you have like you know  
CHS: Right, right  
NB: The, those are guns that when you know, they arrest DC guys in southeast, you know what I'm saying, those are, that's evidence  
CHS: From like, from the drug dealers or something  
NB: And usually they have the best guns, to be honest with you [laughs], they have  
CHS: [Unintelligible]  
NB: They have the best guns

8. When interviewed about this conversation, CHS did not know the identity of the individual referred to by Brankovic as "Jason," referred to hereinafter as Jason LNU. Your affiant believes that Jason LNU may be an employee of the DC Metropolitan Police Department (MPD) based on Brankovic's statements during the call that Jason is a "cop" and he is a "DC guy." There are multiple employees of the DC MPD with the first name Jason. The investigation has yet to confirm Jason LNU's identity.

9. Based on a subsequent identification made by CHS, the individual referred to in the call as "Serge," and described as one of the individuals to whom Jason LNU has previously provided a gun, is believed to be Sergei Kazarian. CHS believes Kazarian is a drug dealer. CHS has this belief based in part on statements CHS heard made by Albert Andrawos, an individual known to CHS to use cocaine, in 2018, after Andrawos received a phone call in CHS's presence. Andrawos complained to CHS, stating something to the effect that these drug dealers act like it is

their full time job. CHS provided law enforcement with the date and time of the telephone call CHS witnessed Andrawos receive. Law enforcement identified the telephone call in Andrawos's historical telephone records. Based on a review of databases available to law enforcement, the phone number that called Andrawos was previously associated with an individual with the same address and last name as Kazarian. CHS also observed Andrawos meet up with Kazarian later that same day.

10. Based on a review of telephone records, it appears Brankovic has had telephonic communications with Kazarian. Telephone records show Brankovic's cell phone, 202-997-5531, and the phone number believed to be associated with Kazarian, in contact as recently as February 13, 2019.

11. The individual referred to as "Layth" in the call is believed to be Layth Mansour, based on other reporting that CHS has provided about Mansour. During the same call, Brankovic told CHS that Layth was involved with bulk shipments of marijuana, but when CHS questioned Brankovic about whether Layth sold "coke" as well as marijuana, Brankovic replied, "mainly weed." Information gathered in a separate and unrelated investigation also suggests that Mansour is involved in illegal drug distribution.

12. Based on the recorded conversation described above, your affiant believes that Jason LNU is a District of Columbia police officer who provided members of the public—possibly including those engaged in illegal drug dealing—firearms obtained in the course of official police activity; and that Brankovic was aware of such exchanges. Notwithstanding Brankovic's statement in the recorded conversation that Jason LNU did not sell the guns, but rather gave them away, your affiant believes that Jason LNU must have received something of

value in exchange for his actions. It is implausible that Jason LNU would risk loss of his job and criminal penalties to “give” members of the public firearms seized in the course of arrests/searches made in the District of Columbia.

13. On September 16, 2018, CHS made another consensually recorded call to Brankovic regarding the status of the gun CHS had requested. The following conversation occurred between CHS and Brankovic:

CHS:...ask that guy, whoever the hell that, um that cop guy is [unintelligible], if he could get something for me that'd be great, I'm telling you, some weird shit happening at my house, just like weird shit like glass breaking, I just, I don't know if they're trying to, somebody trying to break in or whatever, they wouldn't be that stupid because of the, the cameras, but I got to get more cameras too, but you think that guy will get it, the cop guy, or no

NB: Yeah, let me, I'll ask, I'll ask, let me ah, I got to ah

CHS: Just say obviously I can't get one, that kind of shit and whatever

NB: Yeah, I'm not going to even say to him, like if anything like I'll get it and then we'll figure out

CHS: But what's ah, I mean if he gave it to those crack heads before, I mean why the fuck wouldn't he get it for me, you know

NB: Yeah of course, but I haven't seen him in a minute, I haven't seen him in a minute, let me, let me see

CHS: I think, I think I've seen that guy, I think I know who you are talking about, but I'm not sure

NB: Bro if anything like you know we get it from someone else, I got some other people

CHS: Yeah, but I don't want to, I mean it would be better if this if it's more legit

NB: It's the same shit bro, it's, it's bro, it's not legit [laughs], whatever it is, it's not legit

CHS: Alright

NB: Just see what happens

CHS: But, but this guy, I'm saying if he's getting it, it's obviously from

NB: Yeah, yeah, I'll ask, I'll ask around and let you know, what are the options

CHS: But that, but he's always on the street anyway, right, what's his name Jason or something

NB: Yeah

14. Based on Brankovic's statement that, "I got some other people," your affiant believes that Brankovic has communicated with other individuals in addition to Jason LNU regarding the purchase/sale/transfer of illegitimate firearms, and is willing and able to facilitate such illegitimate transfers.

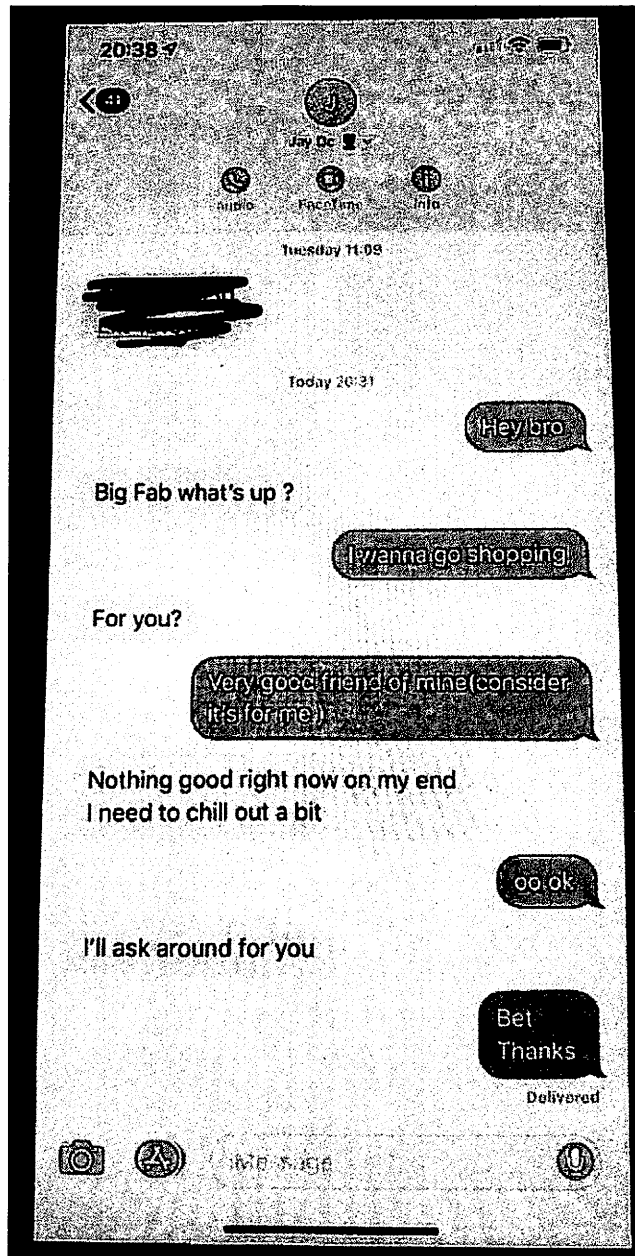
15. The investigation has revealed that both CHS and Brankovic utilize Apple devices, and that their methods of communication include instant messaging via Apple iMessage. On November 16, 2018, at approximately 1:55pm, CHS and Brankovic exchanged the following Apple iMessages:

CHS: Wyd? Anything new with the Jason guy by the way?  
NB: Jason ?  
CHS: Broken glass again fml  
CHS: The cop guy...  
NB: Oooo  
NB: Totally forgot  
NB: Let's me see  
NB: Let\*

16. This conversation continued later on November 16, 2018, at approximately 8:22pm, when they exchanged the following iMessages:

CHS: Try to ask him one day or maybe you can text me with him if you think it's better.  
NB: I'll tell you when I see you  
CHS: Bad?  
NB: Nothing bad  
CHS: I just thought easier to ask him directly if you put me in touch or I can hit him once you talk to him so not bothering u

17. Brankovic replied to this last message by sending CHS a screenshot of Brankovic's communications with another individual who was stored in Brankovic's contacts under the name "Jay Dc" and a police officer emoji, as depicted below:

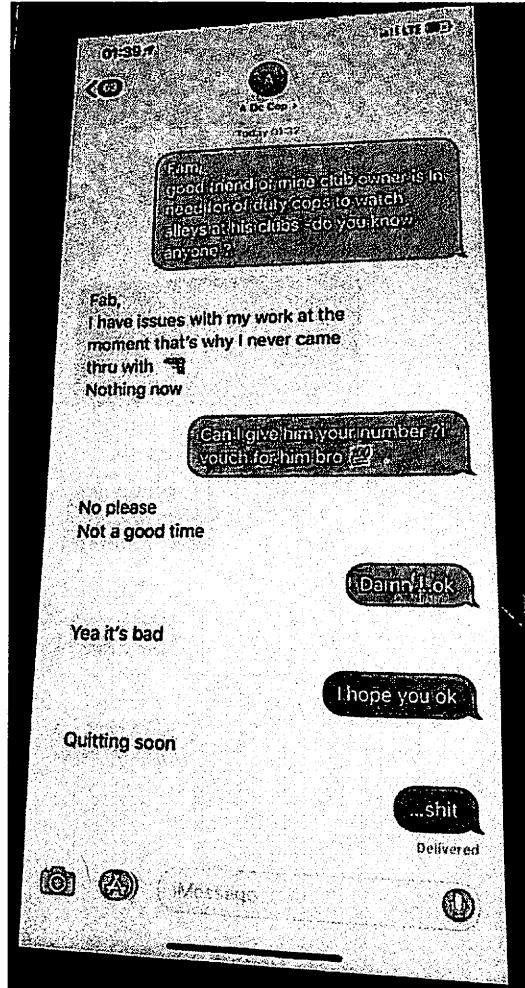


18. Your affiant is aware that when Apple devices exchange iMessages, sent messages appear in blue bubbles, and received messages appear in gray bubbles. When an Apple device exchanges messages with a non-Apple device, there is no iMessage capability and sent messages appear in green bubbles. The screenshot of Brankovic's communications with "Jay

Dc,” in which blue bubbles are depicted, is consistent with Apple iMessaging, with Brankovic as the sender and “Jay Dc” as the recipient.

19. Based on the content of the conversation, the contact name, and the police officer emoji, your affiant believes “Jay Dc” is the same individual previously referenced by Brankovic and known to the investigation as Jason LNU. Based on Jason LNU’s response to Brankovic’s request to go shopping, *i.e.*, “For you?”, your affiant believes that Jason LNU knew what Brankovic meant by shopping—shopping for firearms—because this was not their first discussion about this subject, and that Jason LNU wanted information about who would ultimately receive the weapon. Notably, “shopping” generally involves the activity of *purchasing* goods, suggesting that Brankovic would expect to provide Jason LNU something of value in exchange for a weapon.

20. On January 7, 2019, CHS made two consensually recorded phone calls to Brankovic. In the later January 7, 2019, recorded call, Brankovic mentioned a screenshot of a text message he had previously exchanged with Alex LNU and sent to CHS. That screenshot depicted an exchange that Brankovic had with an individual entered into Brankovic’s contacts as “A. Dc Cop,” whom your affiant believes to be Alex LNU. The screenshot of Brankovic’s communications with “A. Dc Cop.” is depicted below:



As described previously, the blue bubbles are consistent with Apple iMessaging (with Brankovic as the sender and “A. Dc Cop,” believed to be Alex LNU, as the recipient). In the later January 7, 2019, call, Brankovic referenced the text above to indicate that Alex LNU does not currently appear to be in a position to provide CHS with an illegal firearm.

21. During the earlier January 7, 2019 call, Brankovic and CHS discussed the two screenshots Brankovic had sent to CHS and that they were with two different people:

NB: Yeah, I have Jay cop in my phone, but I don't have any

CHS: Bro the one you sent me said Jay cop, look at the screenshot of like

NB: Yeah [laughs] I have them both in my phone, shit bro

...  
NB: So Alex and Jay those are the two cops that I know

....  
NB: I don't know, you see, now when I look at my phone I only have a a screen log with Alex, I don't have, I don't know because it's a new, because I got a phone I don't know, I don't have, I don't have the conversations, I'm trying to see like, I'm going through conversations and trying to see who the fuck is, I'm trying to see conversations with with with Jay, but I don't have, the the the conversation log is clear.

CHS: The one, the one, you sent me a screenshot it says Jay and then a little cop

NB: Give me a second, let me pull it up on my computer, hold on, let me pull it up

After this the call ends and then shortly thereafter there is a follow-up call between Brankovic and CHS on the same date during which Brankovic goes on to say he deleted Alex LNU's number.

22. Although Brankovic claimed to have deleted Alex LNU's number, your affiant believes there is the possibility that Alex LNU's contact information may still be contained on Brankovic's phone accessible by forensic tools, and/or that Alex LNU's contact information may be on Brankovic's computer, as Brankovic asks CHS for a second to pull up the conversation on his computer. As Brankovic claims to have gotten a new phone, he may have an older phone that also could contain Alex LNU's or Jason LNU's contact information. Based on the affiant's experience, individuals tend to retain in their residences prior models of phones and information can at times be extracted from these phones.

23. Brankovic also explained in the later call on January 7, 2019 that Jason LNU "did take care of me, when was it, like, long time ago, right," Brankovic stated that there was another individual, "Alex":

NB: Then, the guy named Alex, also

CHS: Oh I see

NB: Alex, yeah, it's actually Alex, he's better, he's better because like you know like fuckin he's, I told you he got access to like, you know, to all ah, you know when they ah, when they bust whoever they bust when they like, you know, repo, repo their stuff, that's how he gets it from, you know.

CHS: Oh I see

NB: Yeah

CHS: But he's a DC cop too, both of them?

NB: Yeah, both of them.

24. Based on the recorded calls, your affiant believes that in the past, Brankovic may have either facilitated a firearms transfer or personally received a firearm from Jason LNU. Further your affiant believes that Alex, hereinafter referred to as Alex LNU, is another police officer whom Brankovic knew to be willing and able to illicitly provide to members of the public firearms seized in the course of official police activity. The investigation has yet to confirm Alex LNU's identity.

25. Considering Brankovic's use of Apple iMessages in the attempt to obtain a firearm for CHS from police officers Jason LNU and Alex LNU, and Brankovic's statements on recorded calls to the effect that Jason LNU and Alex LNU had provided firearms seized in the course of official police activity to others in the past, and that "Layth" also had firearms, your affiant believes that Brankovic's cell phones and computers contains records of communications relevant to the illegal sale, purchase or transfer of firearms by Jason LNU, Alex LNU, Sergei Kazarian, Nate LNU, Layth Mansour and CHS.

26. On February 12, 2019, Sales and Service Supervisor Djafar Sambou at 2750 Gallows Road, Vienna, Virginia, the building in which the PREMISES is located, was interviewed and advised that based on a review of his lease history, Brankovic has been the sole resident of the PREMISES since approximately September 23, 2017. Sambou advised that

Brankovic's lease does not expire until September 22, 2019. Additionally, Sambou stated that Brankovic has three parking passes, for three different vehicles and that Brankovic's phone number on file with management is 202-997-5531. This is the same phone number on which CHS has had the aforementioned consensually recorded calls with Brankovic.

27. On February 19, 2019, a physical surveillance of the parking garage at 2750 Gallows Road, Vienna, Virginia was conducted. One vehicle observed parked in the garage was registered to Brankovic based on a license plate check. Two other vehicles matching the description of Brankovic's vehicles were also observed parked in the immediate vicinity, although their license plates could not be ascertained from the vantage point of the surveilling agent.

28. On February 22, 2019, another physical surveillance of the parking garage at 2750 Gallows Road, Vienna, Virginia was conducted. Two vehicles matching the description of Brankovic's vehicles were observed parked next to each other in the garage. One of the vehicles, a pickup truck, had the logo for Brankovic's construction company on the driver's side.

29. On February 28, 2019, at approximately 9:30 a.m., an agent observed a male consistent in appearance with Brankovic's license photograph and description entering one of Brankovic's trucks in the parking garage of the building in which the PREMISES is located.

30. The property to be searched includes computers, tablets, and/or mobile phones owned, used, or controlled by Brankovic, including but not limited to an Apple iPhoneX, hereinafter the "Devices."

31. In October 2018, in response to a subpoena requesting information pertaining to Apple accounts associated with Brankovic and telephone number 202-997-5531, Apple provided

records of an Apple account ending in 2360 was created on February 21, 2014 and associated with the Apple ID stefannemanja@icloud.com. The account is listed to Fabio Brankovic 2750 Gallows Rd #401 Vienna, Virginia, day phone 1-202-997-5531. Fabio is Brankovic's nickname. This address is the address listed on Brankovic's Virginia driver's license. Both an iPhone 6 purchased on September 20, 2014, and an iPhone 7 plus purchased on November 18, 2016, are registered to this account. As of the date of the subpoena production, the account status and type was described as an active full iCloud account. An iCloud log provided for this account shows device backup services being used in September 2018 for an iPhone10.3, a.k.a. an iPhone X.

32. Investigators have reason to believe that the Devices are currently located at the PREMISES because this is Brankovic's residence and based on your affiant's training and experience individuals typically keep their current mobile phone on their person and often store older mobile phones no longer in use at their residence. Based on your affiant's training and experience individuals also typically keep their computers at their residence.

33. Further, your affiant submits that the information set forth above establishes probable cause to believe that the Devices contain evidence relevant to the crimes of conspiracy, bribery, and firearms dealing. Based on Brankovic's contacts with CHS, including screenshots of iMessage conversations that Brankovic sent to CHS, there is probable cause to believe that Brankovic uses cell phones to communicate about these crimes. In addition, there is probable cause to believe that the Devices may contain contact information for Jason LNU, Alex LNU, and others involved in the commission of these offenses.

### **TECHNICAL TERMS**

Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

a. “Digital device,” as used herein, includes the following three terms and their respective definitions:

1) A “computer” means an electronic, magnetic, optical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1). Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

2) “Digital storage media,” as used herein, means any information storage device in which information is preserved in binary form and includes electrical, optical, and magnetic digital storage devices. Examples of digital storage media include, but are not limited to, compact disks, digital versatile disks (“DVDs”), USB flash drives, flash memory cards, and internal and external hard drives.

3) “Computer hardware” means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices

(including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

b. “Wireless telephone” (or mobile telephone, or cellular telephone), a type of digital device, is a handheld wireless device used for voice and data communication at least in part through radio signals and also often through “wi-fi” networks. When communicating via radio signals, these telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones, traditional “land line” telephones, computers, and other digital devices. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of applications and capabilities. These include, variously: storing names and phone numbers in electronic “address books”; sending, receiving, and storing text messages, e-mail, and other forms of messaging; taking, sending, receiving, and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; utilizing global positioning system (“GPS”) locating and tracking technology, and accessing and downloading information from the Internet.

c. A “tablet” is a mobile computer, typically larger than a wireless phone yet smaller than a notebook, that is primarily operated by touch-screen. Like wireless phones,

tablets function as wireless communication devices and can be used to access the Internet or other wired or wireless devices through cellular networks, “wi-fi” networks, or otherwise. Tablets typically contain programs called applications (“apps”), which, like programs on both wireless phones, as described above, and personal computers, perform many different functions and save data associated with those functions.

d. A “GPS” navigation device, including certain wireless phones and tablets, uses the Global Positioning System (generally abbreviated “GPS”) to display its current location, and often retains records of its historical locations. Some GPS navigation devices can give a user driving or walking directions to another location, and may contain records of the addresses or locations involved in such historical navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

e. “Computer passwords and data security devices” means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test”

keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

f. “Computer software” means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. Internet Protocol (“IP”) Address is a unique numeric address used by digital devices on the Internet. An IP address, for present purposes, looks like a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 149.101.1.32). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. The “Internet” is a global network of computers and other electronic devices that communicate with each other using numerous specified protocols. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

i. “Internet Service Providers,” or “ISPs,” are entities that provide individuals and businesses access to the Internet. ISPs provide a range of functions for their

customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet, including via telephone-based dial-up and broadband access via digital subscriber line (“DSL”), cable, dedicated circuits, fiber-optic, or satellite. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name, a user name or screen name, an e-mail address, an e-mail mailbox, and a personal password selected by the subscriber. By using a modem, the subscriber can establish communication with an ISP and access the Internet by using his or her account name and password.

j. A “modem” translates signals for physical transmission to and from the ISP, which then sends and receives the information to and from other computers connected to the Internet.

k. A “router” often serves as a wireless Internet access point for a single or multiple devices, and directs traffic between computers connected to a network (whether by wire or wirelessly). A router connected to the Internet collects traffic bound for the Internet from its client machines and sends out requests on their behalf. The router also distributes to the relevant client inbound traffic arriving from the Internet. A router usually retains logs for any devices using that router for Internet connectivity. Routers, in turn, are typically connected to a modem.

l. “Domain Name” means the common, easy-to-remember names associated with an IP address. For example, a domain name of “www.usdoj.gov” refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of

an organization. Examples of first-level, or top-level domains are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and .edu for educational organizations. Second-level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

m. “Cache” means the text, image, and graphic files sent to and temporarily stored by a user’s computer from a website accessed by the user in order to allow the user speedier access to and interaction with that website in the future.

n. “Peer to Peer file sharing” (P2P) is a method of communication available to Internet users through the use of special software, which may be downloaded from the Internet. In general, P2P software allows a user to share files on a computer with other computer users running compatible P2P software. A user may obtain files by opening the P2P software on the user’s computer and searching for files that are currently being shared on the network. A P2P file transfer is assisted by reference to the IP addresses of computers on the network: an IP address identifies the location of each P2P computer and makes it possible for data to be transferred between computers. One aspect of P2P file sharing is that multiple files may be downloaded at the same time. Another aspect of P2P file sharing is that, when downloading a file, portions of that file may come from multiple other users on the network to facilitate faster downloading.

i. When a user wishes to share a file, the user adds the file to shared library files (either by downloading a file from another user or by copying any file into the shared directory), and the file's hash value is recorded by the P2P software. The hash value is independent of the file name; that is, any change in the name of the file will not change the hash value.

ii. Third party software is available to identify the IP address of a P2P computer that is sending a file. Such software monitors and logs Internet and local network traffic.

o. "VPN" means a virtual private network. A VPN extends a private network across public networks like the Internet. It enables a host computer to send and receive data across shared or public networks as if they were an integral part of a private network with all the functionality, security, and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. The VPN connection across the Internet is technically a wide area network (WAN) link between the sites. From a user perspective, the extended network resources are accessed in the same way as resources available from a private network—hence the name "virtual private network." The communication between two VPN endpoints is encrypted and usually cannot be intercepted by law enforcement.

p. "Encryption" is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it but authorized parties can. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an

encryption key, which specifies how the message is to be encoded. Any unintended party that can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key, to which adversaries do not have access.

q. “Malware,” short for malicious (or malevolent) software, is software used or programmed by attackers to disrupt computer operations, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. Malware is a general term used to refer to a variety of forms of hostile or intrusive software.

#### **COMPUTERS, ELECTRONIC/MAGNETIC STORAGE, AND FORENSIC ANALYSIS**

34. As described above and in Attachment B, this application seeks permission to search for evidence, fruits, contraband, instrumentalities, and information that might be found on the PREMISES, in whatever form they are found. One form in which such items might be found is data stored on one or more digital devices. Such devices are defined above and include any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and

security devices. Thus, the warrant applied for would authorize the seizure of digital devices or, potentially, the copying of stored information, all under Rule 41(e)(2)(B). Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that, if digital devices are found on the PREMISES, there is probable cause to believe that the items described in Attachment B will be stored in the Device(s) for at least the following reasons:

a. Individuals who engage in criminal activity, including violations of bribery, conspiracy and/or firearms dealing use digital devices to communicate with co-conspirators; to store on digital devices, like the Devices, documents and records relating to their illegal activity, which can include photos, copies of communications with co-conspirators; contact information of co-conspirators, including telephone numbers, email addresses, identifiers for social medial accounts; and records of illegal transactions, to, among other things, (1) keep track of co-conspirator's contact information; (2) keep a record of illegal transactions for future reference; (3) keep an accounting of illegal proceeds for purposes of, among other things, and splitting those proceeds with co-conspirators. In this case, as described above, Brankovic used iMessages to communicate with Jason LNU and Alex LNU and then send copies of these communications to CHS.

b. Individuals who engage in the foregoing criminal activity, in the event that they change digital devices, will often "back up" or transfer files from their old digital devices to that of their new digital devices, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

c. Digital device files, or remnants of such files, can be recovered months or even many years after they have been downloaded onto the medium or device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person “deletes” a file on a digital device such as a home computer, a smart phone, or a memory card, the data contained in the file does not actually disappear; rather, that data remains on the storage medium and within the device unless and until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the digital device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve “residue” of an electronic file from a digital device depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer, smart phone, or other digital device habits.

35. As further described in Attachment B, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes described in this affidavit, but also for forensic electronic evidence or information that

establishes how the digital device(s) were used, the purpose of their use, who used them (or did not), and when. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit there is probable cause to believe that this forensic electronic evidence and information will be in any of the Device(s) at issue here because:

a. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or texting files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the digital device(s) are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole. Digital data stored in the Device(s), not currently associated with any file, can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on a hard drive that show what tasks and processes on a digital device were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smart phone, or other

digital device was in use. Computer, smart phone, and other digital device file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

b. Forensic evidence on a digital device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, chats, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time, and potentially who did not.

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how such digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital device evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on digital devices is evidence may depend on other information stored on the devices and the application of knowledge about how

the devices behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on the device. For example, the presence or absence of counter-forensic programs, anti-virus programs (and associated data), and malware may be relevant to establishing the user's intent and the identity of the user.

f. I know that when an individual uses a digital device to commit bribery and/or firearms dealing, the individual's device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a digital device used to commit a crime of this type may contain data that is evidence of how the digital device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense and the identities of those perpetrating it.

#### **METHODS TO BE USED TO SEARCH DIGITAL DEVICES**

36. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time, in part because there are so many types of digital devices and software programs in use today. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Recovery of “residue” of electronic files from digital devices also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is often essential to conducting a complete and accurate analysis of data stored on digital devices.

c. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows

someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.

d. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear as though the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting “keyword” search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format (“PDF”), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography, a digital device

user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband, or instrumentalities of a crime.

e. Analyzing the contents of mobile devices, including tablets, can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as “AES-256 encryption” to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, “Hide It Pro,” disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

f. Based on all of the foregoing, I respectfully submit that searching any digital device for the information, records, or evidence pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the devices. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.

37. The volume of data stored on many digital devices will typically be so large that it will be extremely impractical to search for data during the physical search of the premises.

a. Therefore, in searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this search warrant will employ the following procedures:

1. Upon securing the PREMISES, law enforcement personnel will, consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, seize any digital devices (that is, the Device(s)), within the scope of this warrant as defined above, deemed capable of containing the information, records, or evidence described in Attachment B and transport these items to an appropriate law enforcement laboratory or similar facility for review. For all the reasons described above, it would not be feasible to conduct a complete, safe, and appropriate search of any such digital devices at the PREMISES. The digital devices, and/or any digital images thereof created by law enforcement sometimes with the aid of a technical expert,

in an appropriate setting, in aid of the examination and review, will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachment B.

2. The analysis of the contents of the digital devices may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by “opening,” reviewing, or reading the images or first few “pages” of such files in order to determine their precise contents; “scanning” storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic “keyword” searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

3. In searching the digital devices, the forensic examiners may examine as much of the contents of the digital devices as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic examiners may search for and attempt to recover “deleted,” “hidden,” or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the seized digital devices will be specifically chosen to identify the specific items to be seized under this warrant.

**BIOMETRIC ACCESS TO DEVICE(S)**

38. This warrant permits law enforcement agents to obtain from the person of Nemanja Brankovic (but not any other individuals present at the PREMISES at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person(s)' physical biometric characteristics will unlock the Device(s). The grounds for this request are as follows:

39. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

40. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors

found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

41. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

42. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

43. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's

contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

44. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices, the Device(s), will be found during the search. The passcode or password that would unlock the Device(s) subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the Device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

45. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

46. Due to the foregoing, if law enforcement personnel encounter any Device(s) that are subject to seizure pursuant to this warrant and may be unlocked using one of the


aforementioned biometric features, this warrant permits law enforcement personnel to obtain from the aforementioned person(s) the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s), including to (1) press or swipe the fingers (including thumbs) of the aforementioned person(s) to the fingerprint scanner of the Device(s) found at the PREMISES; (2) hold the Device(s) found at the PREMISES in front of the face of the aforementioned person(s) to activate the facial recognition feature; and/or (3) hold the Device(s) found at the PREMISES in front of the face of the aforementioned person(s) to activate the iris recognition feature, for the purpose of attempting to unlock the Device(s) in order to search the contents as authorized by this warrant.

47. The proposed warrant does not authorize law enforcement to require that the aforementioned person(s) state or otherwise provide the password, or identify specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the Device(s). Nor does the proposed warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) would be permitted under the proposed warrant. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person(s) for the password to any Device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device(s), the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

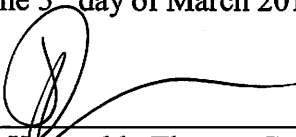
**CONCLUSION**

48. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and to seize the items described in Attachment B.

Respectfully submitted,

  
\_\_\_\_\_  
Jeffrey Scott  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me  
on the 5<sup>th</sup> day of March 2019.

  
\_\_\_\_\_  
Theresa Carroll Buchanan  
United States Magistrate Judge  
The Honorable Theresa Carroll Buchanan  
United States Magistrate Judge  
Alexandria, Virginia

**ATTACHMENT A**

*Property to be searched*

The property to be searched is 2750 Gallows Road Apartment 401, Vienna, Virginia (the “PREMISES”), further described as an apartment on the fourth floor of an apartment building. The apartment itself has a brown door with the number 401 on the wall to the left of the door. The apartment building has the name “AVALON” above the main entrance and on the glass wall next to the main entrance below the number 2750.



**ATTACHMENT B**

*Property to be seized*

1. The items to be seized are fruits, evidence, information, contraband, or instrumentalities, in whatever form and however stored, relating to violations of Title 18 United States Code Sections 201, 371, and 922 as described in the search warrant affidavit, including, but not limited to:

- a. Records and information relating to firearm(s) and/or gun(s), purchasers of firearm(s) and/or gun(s), and/or suppliers of firearm(s) and/or gun(s) including but not limited to firearm(s) and/or gun(s) themselves and/or photo(s) of firearm(s) and/or gun(s).
- b. Records and information relating to law enforcement officer(s) or employee(s) of a law enforcement agency/department;
- c. Records and information relating to the contact Jay Dc (believed to be Jason Last Name Unknown (LNU)), the contact A. Dc Cop (believed to be Alex LNU), Jason LNU, Alex LNU, Serge LNU (believed to be Sergei Kazarian), Nate LNU, or Layth LNU (believed to be Layth Mansour);
- d. Records and information relating to the identity or location of perpetrators, aiders and abettors, coconspirators, and accessories after the fact;
- e. Records and information that constitute evidence of use, control, ownership, or occupancy of the PREMISES and things therein;
- f. Records and information that constitute evidence of the state of mind of Nemanja Brankovic, Jason LNU, Alex LNU, Serge LNU (believed to be Sergei Kazarian),

Nate LNU, and/or Layth LNU (believed to be Layth Mansour), *e.g.*, attempts to delete communications and/or contact information, intent, absence of mistake, or evidence indicating preparation or planning, or knowledge and experience, related to the criminal activity under investigation; and

- g. Records and information that constitute evidence concerning persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with Nemanja Brankovic, Jason LNU, Alex LNU, Serge LNU (believed to be Sergei Kazarian), Nate LNU, and/or Layth LNU (believed to be Layth Mansour), about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts.

2. Digital devices used in the commission of, or to facilitate, the above described offenses, including facilitating or attempting to facilitate the illegal transfer of firearms in violation of 18 U.S.C. § 922.

3. For any digital device which is capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities as described in the search warrant affidavit and above, hereinafter the “Device(s)”:

- a. evidence of who used, owned, or controlled the Device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, chat, instant messaging logs, photographs, and correspondence;

- b. evidence of software, or the lack thereof, that would allow others to control the Device(s), such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the attachment to the Device(s) of other storage devices or similar containers for electronic evidence;
- d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Device(s);
- e. evidence of the times the Device(s) was used;
- f. passwords, encryption keys, and other access devices that may be necessary to access the Device(s);
- g. documentation and manuals that may be necessary to access the Device(s) or to conduct a forensic examination of the Device(s);
- h. records of or information about Internet Protocol addresses used by the Device(s);
- i. records of or information about the Device(s)'s Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
- j. Information that constitutes evidence concerning persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with the

Account about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts;

- k. Information that constitutes evidence indicating the Account user's state of mind, *e.g.*, attempts to delete communications and/or contact information, intent, absence of mistake, or evidence indicating preparation or planning, related to the criminal activity under investigation;
- l. Information that constitutes evidence concerning how and when the Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the Account user;
- m. Records and information (to include iMessages, SMS messages, MMS messages, instant messages, emails, including stored or preserved copies of communications (including all draft and deleted messages and deleted contacts)) relating to:
  - i. Firearm(s) and/or gun(s), purchasers of firearm(s) and/or gun(s), and/or suppliers of firearm(s);
  - ii. Photo(s) of firearm(s) and/or gun(s);
  - iii. Photo(s) of law enforcement officer(s) or employee(s) of a law enforcement agency/department;
  - iv. Photo(s) of Jay Dc (believed to be Jason Last Name Unknown (LNU)), A. Dc Cop (believed to be Alex LNU), Jason LNU, Alex LNU, Serge LNU (believed to be Sergei Kazarian), Nate LNU, or Layth LNU (believed to be Layth Mansour);

- v. Communications with, including, and/or about Jay Dc (believed to be Jason Last Name Unknown (LNU)), A. Dc Cop (believed to be Alex LNU), Jason LNU, Alex LNU, Serge LNU (believed to be Sergei Kazarian), Nate LNU, or Layth LNU (believed to be Layth Mansour);
- vi. Communications with current and/or former employee(s) of the District of Columbia Metropolitan Police Department;
- vii. Communications with, including, and/or about law enforcement officer(s), or employee(s) of a law enforcement agency/department;
- viii. The solicitation, request, offer, promise, gift, provision, demand, acceptance, or receipt of any bribes, or any agreement related thereto;
- ix. The identity and/or location of perpetrators, aiders and abettors, and co-conspirators;
- x. Names, addresses, telephone numbers, e-mail addresses, social media accounts, and any other user profiles of perpetrators, aiders and abettors and co-conspirators; and
- xi. Any motive for committing the above named offenses.

4. During the execution of the search of the PREMISES described in Attachment A, law enforcement personnel are also specifically authorized to obtain from Nemanja Brankovic (but not any other individuals present at the PREMISES at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock any Device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable

suspicion that the aforementioned person(s)' physical biometric characteristics will unlock the Device(s), to include pressing fingers or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition of:

- (a) any of the Device(s) found at the PREMISES,
- (b) where the Device(s) are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the Device(s)'s security features in order to search the contents as authorized by this warrant.

5. While attempting to unlock the device by use of the compelled display of biometric characteristics pursuant to this warrant, law enforcement is not authorized to demand that the aforementioned person(s) state or otherwise provide the password or identify the specific biometric characteristics (including the unique finger(s) or other physical features), that may be used to unlock or access the Device(s). Nor does the warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) is permitted. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person(s) for the password to any Device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device(s), the agents will not state or otherwise imply that the warrant requires the person to

provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

6. As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

7. The term “digital devices” includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); security devices; and any other type of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions.